ORIGINAL

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ❒ Original ❒ Duplicate Original

UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Storage unit No. J21, located at Highway 22 Storage, 130 50th Ave. NW, Salem, OR 97304, as described in Attachment A	)	Case No. 3:25-mc-00476

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of Oregon
(identify the person or describe the property to be searched and give its location):

Storage unit No. J21, located at Highway 22 Storage, 130 50th Ave. NW, Salem, OR 97304, as described in Attachment A hereto.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

YOU ARE COMMANDED to execute this warrant on or before May 12, 2025 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ❒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Magistrate Judge Beckerman, via clerk .
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____ .

Date and time issued: 4/28/2025 10:33 am

Stacie F. Beckerman
Judge's signature

City and state: Portland, Oregon Hon. Stacie F. Beckerman, U.S. Magistrate Judge
Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
3:25-mc-00476	4-28-25 at 12:45 p.m.	In the unit w/ manager

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Zero items were found. The unit was completely empty.

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 4/28/25

Executing officer's signature

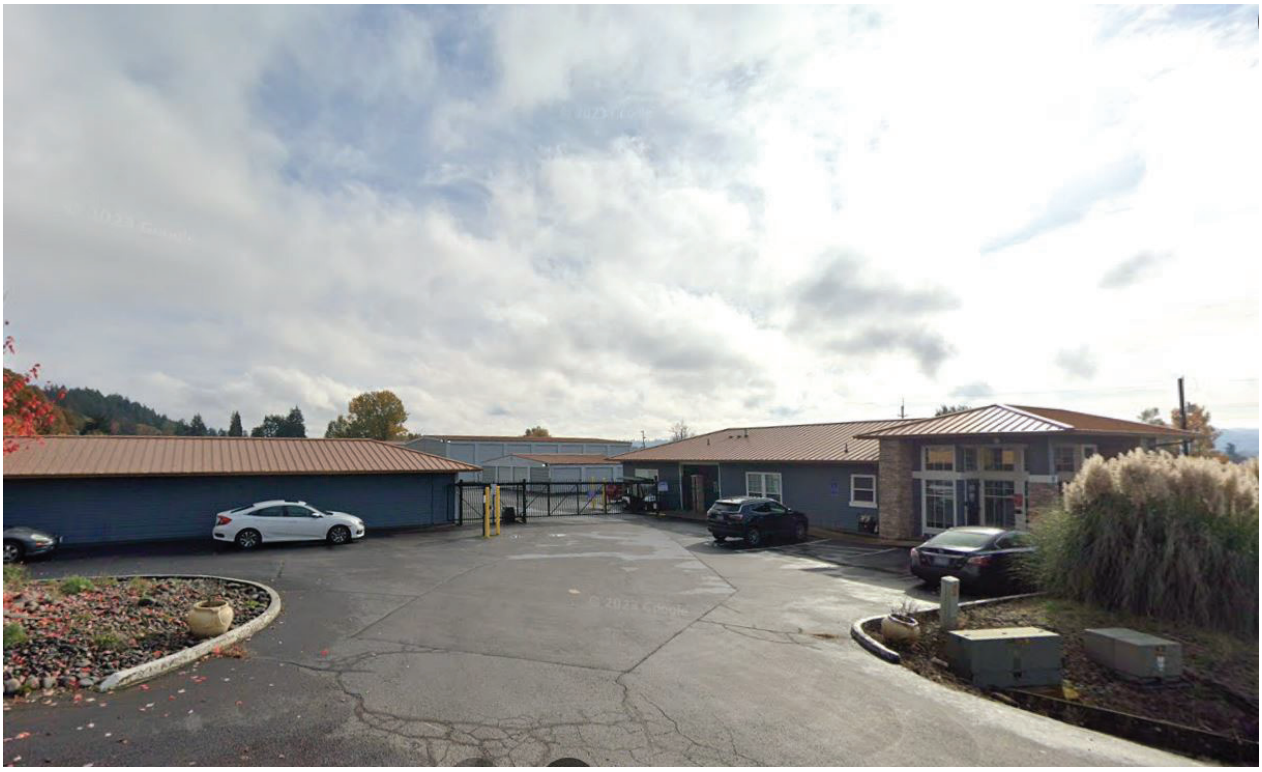
SA Jeffrey Thomas, DEA

Printed name and title

ATTACHMENT A

Property to Be Searched

The property to be searched is Storage unit No. J21, located at Highway 22 Storage, 130 50th Ave. NW, Salem, OR 97304, identified as the "**Subject Premises**." The **Subject Premises** is further described as a 10 foot by 20 foot storage unit labeled J21 within the secured area of the business named Highway 22 Storage. (See below photo of the Highway 22 Storage facility).



ATTACHMENT B

Items to Be Seized

The items to be searched for, seized, and examined, are those items on the premises located at Storage unit No. J21, Highway 22 Storage, 130 50th Ave. NW, Salem, OR 97304 ("**Subject Premises**"), referenced in Attachment A, that contain evidence, contraband, fruits, and instrumentalities of violations of Title 21 U.S.C. §§ 841(a)(1) and 846, Possession with the Intent to Distribute a Controlled Substance and Conspiracy to Possess with the Intent to Distribute a Controlled Substance, make it illegal to possess with intent to distribute a Controlled Substance, or to conspire to do so. Title 21, United States Code, Section 843(b) makes it unlawful to use a communication facility, such as a cellular telephone, to distribute controlled substances. The items to be seized cover the period of January 1, 2024, through the date of the execution of the warrant.

1. The items referenced above to be searched for, seized, and examined are:

a. Controlled substances, including but not limited to methamphetamine, fentanyl or cocaine, held in violation of 18 U.S.C 1956 and 21 U.S.C. Sections 841(a)(1) and 846;

b. Firearms, firearm accessories, and other dangerous weapons and ammunition;

c. Financial profits, proceeds and instrumentalities of trafficking in narcotics and money laundering, including U.S. Currency and other items of value.

d. Paraphernalia for packaging, smuggling, processing, diluting, manufacturing, weighing, and distributing controlled substances, for example: hidden compartments, scales, blenders, funnels, sifters, grinders, glass panes, mirrors, razor blades, plastic bags, heat sealing devices, and dilutants such as inositol, vitamin B12, etc.;

e. Books, records, receipts, notes, ledgers, and other documents relating to the manufacture and distribution of controlled substances; money laundering, communications between members of the conspiracy, and evidence of the use of apparently legitimate businesses to disguise profits.

f. Personal books and papers reflecting names, addresses, telephone numbers, and other contact or identification data relating to the manufacture, importation and distribution of controlled substances, and money laundering.

g. Financial records relating to controlled substances income and expenditures of money and wealth, to wit: money orders, wire transfer records, cashier's checks and receipts, account records, passbooks, tax records, safe deposit box keys and records, checkbooks, and check registers, as well as precious metals and gems such as gold, silver, diamonds, etc. purchased/acquired between January 1, 2024, and the present;

h. Items of personal property that tend to identify the person(s) in residence, occupancy, control, or ownership of the premises, including but not limited to canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, utility and telephone bills, statements, identification documents, and keys;

j. Other cellular telephones, computers and other electronic devices capable of storing data that constitutes evidence or the instrumentality of drug dealing and conspiracy to do the same may be seized so the government may apply for search warrants for any other devices located at the **Subject Premises**;

k. Latent prints and identifying material from items at the premises, including the fingerprints of the unidentified individuals located at the **Subject Premises**.

2. As used in this attachment, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant and any computer, storage medium, or digital device that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter "Computer"):

a. Evidence of who used, owned, or controlled the Computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence.

b. Evidence of software that would allow others to control the Computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

c. Evidence of the lack of such malicious software.

d. Evidence indicating how and when the Computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime under investigation and to the Computer user.

e. Evidence indicating the Computer user's state of mind as it relates to the crime under investigation.

f. Evidence of the attachment to the Computer of other storage devices or similar containers for electronic evidence.

g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Computer.

h. Evidence of the times the Computer was used.

i. Passwords, encryption keys, and other access devices that may be necessary to access the Computer.

j. Documentation and manuals that may be necessary to access the Computer or to conduct a forensic examination of the Computer.

k. Records of or information about Internet Protocol addresses used by the Computer.

l. Records of or information about the Computer's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

m. Contextual information necessary to understand the evidence described in this attachment.

Search Procedure

4. The search for data capable of being read, stored, or interpreted by a computer or storage device, may require authorities to employ techniques, including imaging any computer or storage media and computer-assisted scans and searches of the computers and storage media, that might expose many parts of the computer to human inspection in order to determine whether it constitutes evidence as described by the warrant.

5. The initial examination of the computer and storage media will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

6. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the computer and storage media do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

7. If an examination is conducted, and the computer and storage media do not contain any data falling within the ambit of the warrant, the government will return the computer and storage media to its owner within a reasonable period of time following the search and will seal any image of the computer and storage media, absent further authorization from the Court.

8. The government may retain the computer and storage media as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the computer and storage media and/or the data contained therein.

9. The government will retain a forensic image of the computer and storage media for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.